AO93 Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
District of Arizona

In the Matter of the Search of
8563 West Mission Lane, Peoria, Arizona, 85345.

Case No. 23-3169MB

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the District of Arizona:

As further described in Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal:

As set forth in Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 4/21/23 *(not to exceed 14 days)*
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to any United States Magistrate Judge on criminal duty in the District of Arizona.

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized ☐ for 30 days (*not to exceed 30*) ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 4/7/23 @9:40AM

M Morrissey
Judge's signature

City and state: Phoenix, Arizona

Honorable Michael T. Morrissey, U.S. Magistrate Judge
Printed name and title

AO 93 (Rev. 01/09) Search and Seizure Warrant (Page 2)

RETURN

Case No.:	Date and Time Warrant Executed:	Copy of warrant and inventory left with:

Inventory Made in the Presence of:

Inventory of the property taken and name of any person(s) seized:

CERTIFICATION

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Property to be searched

The property to be searched is the residence of FARIBORZ ABBASI ("ABBASI") and ALEXANDRA MORALES ("MORALES) located at 8563 West Mission Lane, Peoria, Arizona, 85345 ("PREMISES"), further described as follows:

PREMISES is a single family home built on or about 1997, with approximately 1,323 square feet and a lot size of approximately 5,227 square feet. The property has a tan colored stucco exterior, with tan and red colored tile roofing. The property has a two car garage door on the right side of the property with a concrete driveway. The garage is attached to the home. In the front of the home, there is a small yard with rock gravel and a palm tree located on the right side of the driveway.

PREMISES includes any other means of storage on the property or its curtilage, including storage containers and vehicles. Several pictures of the PREMISES to be searched are below:

ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1344 (Bank Fraud), 18 U.S.C. § 371 Conspiracy, and 18 U.S.C. 1957(a) (Money Laundering), and those violations involving FARIBORZ ABBASI ("ABBASI") and ALEXANDRA MORALES ("MORALES") and occurring after January 1, 2019, including:

a. All documents and communications referring or relating to Paycheck Protection Program ("PPP") loan applications and/ or the Small Business Administration ("SBA") Economic Impact Disaster Loan ("EIDL") applications or documents;

b. Any communications regarding PPP loans and/or SBA EIDLs, including loans, applications, communications with bank representatives, and communications with SBA representatives;

c. Records pertaining to business structure or ownership, including articles of incorporation, stock certificates, and business cards; of Italian Brothers Pizza LLC, American Union Professional Services LLC, Also Known As ("AKA") American Union Professional and Landscape Services LLC and American Union Professional, Price Match Mattress and Furniture LLC, Power Health Management LLC, Rocky Point Restaurant and Bar LLC, and World Buffett LLC (collectively, "ABBASI's and MORALES' BUSINESSES").

d. Any documents and/or communication containing tax information for ABBASI, MORALES, and/or ABBASI's and MORALES' BUSINESSES, including tax returns and Forms 940 and 941 from January 1, 2019, to the present;

e. Communications regarding profit and loss statements and/or depreciation calculations for ABBASI, MORALES and/or ABBASI's and MORALES' BUSINESSES, from January 1, 2019, to the present;

f. All financial records, including but not limited to bank records, and records concerning employee lists and clients for ABBASI, MORALES, and/or ABBASI's and MORALES' BUSINESSES from January 1, 2019, to the present;

g. Records pertaining to wealth and the movement of wealth since 2020 for ABBASI, MORALES, and/or ABBASI's and MORALES' BUSINESSES, such as brokerage and financial institution statements, wire transfers, currency exchanges, deposit slips, cashiers' checks, and/or other financial documents related to depository bank accounts, lines of credit, credit card accounts, real estate mortgage initial purchase loans or loan refinances, residential property leases, escrow accounts, the purchase, sale, or leasing of automobiles or real estate, or auto loans, and investments, or showing or referring to purchases or transactions for more than $5,000;

h. United States and foreign currency in excess of 5,000.00; precious metals and jewelry; wire transfers, cashier checks, money orders, and other financial instruments or items of value;

i. Records, documents, programs, applications or materials pertaining to business or merchant accounts for ABBASI, MORALES, and/or ABBASI's and MORALES' BUSINESSES;

j. Documents pertaining to U.S. Post Office Boxes, public storage units, rental cars, safety deposit boxes, Commercial Mail Receiving Agencies, building or office space, or receiving mail for ABBASI, MORALES, and/or ABBASI's and MORALES' BUSINESSES;

k. Any communications and/or other correspondence regarding financial institution fraud and wire fraud, including any stored or deleted communications;

l. With respect to any storage medium or digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

    i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted;

    ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

    iii. evidence of the attachment of other devices;

    iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

    v. evidence of the times the device was used;

vi. applications, programs, software, documentation, manuals, passwords, keys, and other access devices that may be necessary to access the device or data stored on the device, to run software contained on the device, or to conduct a forensic examination of the device;

vii. records of or information about Internet Protocol addresses used by the device.

viii. records of or information about the devices' Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

2. As used herein, the terms "records," "information," "documents," "programs," "applications," and "materials" include records, information, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as mobile telephones, and smart phones; storage media, such as hard disk drives and portable hard drives, memory cards, USB drives, or other type of portable data storage device used with digital devices.

Search Procedure for Digital Devices

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

    i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the scope of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of items to be seized.

    ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase," "Griffeye," and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

d. If the search determines that a digital device does not contain any data falling within the scope of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the scope of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the scope of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

6. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.